IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Victor Cho, Giovanni Stewart, and David L'Abbe, individually and on behalf of all others similarly situated, Plaintiffs, v. CBS Interactive, Inc., Defendant.	Civil Action No. 1:24-cv-08312-JPO **FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Victor Cho, Giovanni Stewart and David L'abbe ("Plaintiffs") bring this action on behalf of themselves and all others similarly situated against CBS Interactive Inc. ("Defendant"). Plaintiffs make the following allegations pursuant to the investigation of their counsel based upon information and belief, except to the allegations specifically pertaining to themselves, which is based on their personal knowledge.

NATURE OF THE ACTION

1. Defendant CBS Interactive Inc. ("Defendant" or "Paramount") is one of the largest pre-recorded video content providers in the United States. Defendant owns and operates its online and mobile streaming applications ("Apps"), including www.paramountplus.com (the "Website"). Unbeknownst to Plaintiffs and the Class Members, Defendant employed Facebook, TikTok, and Taboola, among other third parties, to intercept and disclose consumers' search terms, video watching information, and personally identifiable information without seeking or obtaining their consent.. In so doing, Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710, *et seq.* the Federal Wiretap Act ("Wiretap Act"), 18 U.S.C. § 2710, *et seq.*, and the California

Information Privacy Act ("CIPA"), § 631, *et seq.*

JURISDICTION AND VENUE

2. This Court has original jurisdiction under 28 U.S.C. § 1331 based on Plaintiffs' claims under the Video Privacy Protection Act, 18 U.S.C. § 2710, *et seq* and the Federal Wiretap Act, 18 U.S.C. § 2511(1) (a)-(e). This Court also has subject matter jurisdiction over this lawsuit under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because this is a proposed class action in which: (1) there are at least 100 Class Members; (2) the combined claims of Class Members exceed $5,000,000, exclusive of interest, attorneys' fees, and costs; and (3) Defendant and at least one Class member are domiciled in different states.

3. This Court has general jurisdiction over Defendant because Defendant maintains its principal place of business within this District.

4. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because Defendant resides in this District and a substantial part of the events giving rise to Plaintiffs' claims took place within this District.

PARTIES

5. Plaintiff Victor Cho is a citizen of California, who resides in Pasadena, California. Plaintiff Cho has had an account with Paramount which he has used to stream shows and movies from his computer on a regular basis within the last two years since the filing of this Complaint. Throughout the duration of his interactions with Defendant's Website, Plaintiffs Cho has maintained and used his Facebook account from the same browser that he used to request and view Paramount video content on the Website.

6. During that time, Mr. Cho: (a) accessed the Website; (b) had a Facebook profile that could be accessed by members of the public and that included his name and photograph; (c)

logged into his Facebook account; and (d) searched for, clicked on, and watched pre-recorded videos on the Website.

7. Pursuant to the systematic process described herein, Defendant caused Mr. Cho's video consumption to be sent along with his personally identifiable information ("PII") and other persistent cookies and trackers (including his IP address) to Facebook, TikTok, and Taboola (collectively, the "Tracking Entities") without his knowledge or consent each time he requested and viewed video content through the Website.

8. Mr. Cho never consented, agreed, nor otherwise permitted Defendant to disclose his PII and viewing information to the Tracking Entities and certainly did not do so for purposes violative of the VPPA, the Wiretap Act, or CIPA.

9. Plaintiff Giovanni Stewart is a citizen of California, who resides in Mission Viejo, California. Plaintiff Stewart has had an account with Paramount which he has used to stream shows and movies from his computer Fall of 2021. Throughout the duration of his interactions with Defendant's Website, Plaintiff Stewart has maintained and used his Facebook account from the same browser that he used to request and view Paramount video content on the Website.

10. During that time, Mr. Stewart: (a) accessed the Website; (b) had a Facebook profile that could be accessed by members of the public and that included his name and photograph; (c) logged into his Facebook account; and (d) searched for, clicked on, and watched pre-recorded videos on the Website.

11. Pursuant to the systematic process described herein, Defendant caused Mr. Stewart's video consumption to be sent along with his PII and other persistent cookies and trackers (including his IP address) to Facebook, TikTok, and Taboola (collectively, the "Tracking Entities") without his knowledge or consent each time he requested and viewed video

content through the Website.

12. Mr. Stewart never consented, agreed, nor otherwise permitted Defendant to disclose his PII and viewing information to the Tracking Entities and certainly did not do so for purposes violative of the VPPA, the Wiretap Act, or CIPA.

13. Plaintiff David L'Abbe is a citizen of California, who resides in Sonora, California. Plaintiff L'Abbe has had an account with Paramount which he has used to stream shows and movies from his computer since Fall of 2021. Throughout the duration of his interactions with Defendant's Website, Plaintiff L'Abbe has maintained and used his Facebook account from the same browser that he used to request and view Paramount video content on the Website.

14. During that time, Mr. L'Abbe: (a) accessed the Website; (b) had a Facebook profile that could be accessed by members of the public and that included his name and photograph; (c) logged into his Facebook account; and (d) searched for, clicked on, and watched pre-recorded videos on the Website.

15. Pursuant to the systematic process described herein, Defendant caused Mr. L'Abbe's video consumption to be sent along with his PII and other persistent cookies and trackers (including his IP address) to the Tracking Entities without his knowledge or consent each time he requested and viewed video content through the Website.

16. Mr. L'Abbe never consented, agreed, nor otherwise permitted Defendant to disclose his PII and viewing information to the Tracking Entities and certainly did not do so for purposes violative of the VPPA, the Wiretap Act, or CIPA.

17. Defendant CBS Interactive, Inc. is a Delaware corporation with its principal place of business located at 1515 Broadway New York, New York 10036.

GENERAL ALLEGATIONS

I. History and Overview of the VPPA

18. The impetus for the VPPA began with President Ronald Reagan's nomination of Judge Robert Bork to the United States Supreme Court. During the confirmation process, a movie rental store disclosed the nominee's rental history to the Washington City Paper which then published that record. Congress responded by passing the VPPA, with an eye toward the digital future. As Senator Patrick Leahy, who introduced the Act, explained:

> "It is nobody's business what Oliver North or Pratik Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home. In an area of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. I think that is wrong".

S. Rep. 100-599, at 5-6 (internal ellipses and brackets omitted).

19. In 2012, Congress amended the VPPA, and in so doing, reiterated the Act's applicability to "so-called 'on-demand' cable services and Internet streaming services [that] allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones." S. Rep. 112-258, at 2.

20. The VPPA prohibits "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1).

21. The VPPA defines personally identifiable information ("PII") as "information which identifies a person as having requested or obtained specific video materials or services

from a video tape service provider." 18 U.S.C. § 2710(a)(3).

22. A video tape service provider is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

23. Individuals who are "aggrieved" by a violation of the VPPA may bring an action for "not less than liquidated damages" of $2,500 per violation, in addition to other remedies. 18 U.S.C. §§ 2710(c)(1)-(2).

II. History and Overview of the Federal Wiretap Act

24. Congress enacted The Federal Wiretap Act "as a response to Fourth Amendment concerns surrounding the unbridled practice of wiretapping to monitor telephonic communications."[1]

25. The Wiretap Act primarily concerned the government's use of wiretaps but was amended in 1986 through the Electronic Communications Privacy Act ("ECPA") to provide a private right of action for private intrusions as though they were government intrusions.[2]

26. Congress was concerned that technological advancements like "large-scale mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing"[3] were rendering the Wiretap Act out-of-date. Congress amended the Wiretap Act in 1986 through the Electronic Communications Privacy Act ("ECPA") to provide a private right of action for private intrusions as though they were government intrusions.

---

[1] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022), https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1541&context=crsj

[2] *Id.*

[3] Senate Rep. No. 99-541, at 2 (1986).

27. As a result, the ECPA primarily focused on two types of computer services that were prominent in the 1980s: (i) electronic communications like email between users; and (ii) remote computing services like cloud storage or third-party processing of data and files. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014).

28. Title I of the ECPA amended the Wiretap Act such that a violation occurs when a person or entity: (i) provides an electronic communication service to the public; and (ii) intentionally divulges the contents of any communication; (iii) while the communication is being transmitted on that service; (iv) to any person or entity other than the intended recipient of such communication.

29. While the ECPA allows a single party to consent to the interception of an electronic communication, single party consent is only acceptable where the communication is not "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. §2511(2)(d).

III. History and Overview of The CIPA

30. The California Legislature enacted the Invasion of Privacy Act to protect certain privacy rights of California citizens. The legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

31. The California Supreme Court has repeatedly stated the "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone or listen in on the call*." Ribas v. Clark*, 38 Cal. 3d 355, 363 (1985) (emphasis added, internal quotations omitted). This restriction

is based on the "substantial distinction … between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device." *Id.* at 361 (emphasis added). Such "simultaneous dissemination" "denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements." *Id.*; s*ee also U/S. Dept. of Justice v. Reporters Committee for Freedom of Press*, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

32. As part of CIPA, the California Legislature introduced § 631(a), which prohibits any person or entity from (i) "intentionally tap[ping], or mak[ing] any unauthorized connection … with any telegraph or telephone wire," (ii) "willfully and without the consent of all parties to the communication … read[ing], or attempt[ing] to read, or to learn the contents or meaning of any … communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within [California]," or (iii) "us[ing], or attempt[ing] to use … any information so obtained." These are "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). CIPA § 631(a) also penalizes those who "aid[], agree[] with, employ[], or conspire[] with any person" who conducts the aforementioned wiretapping.

33. The California Legislature also enacted CIPA § 638.51(a), which prohibits any person or entity from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

34. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire

or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b). A "trap and trace device" is a "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(b).

35. In plain English, a "pen register" is a "device or process" that records outgoing information, while a "trap and trace device" is a "device or process" that records incoming information. "[T]he California Supreme Court has also emphasized that all CIPA provisions are to be interpreted in light of the broad privacy-protecting statutory purposes of CIPA." *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022). "Thus, when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

36. Individuals may bring an action against the violator of any provision of CIPA for $5,000 per violation. Cal. Penal Code § 637, *et seq.*

IV. Defendant's Website and Tracking Tools

A. Overview of How Websites Operate

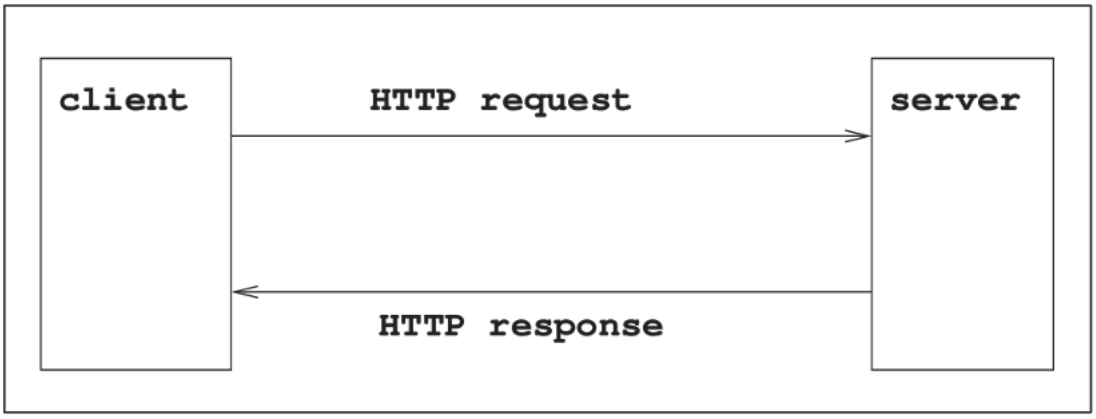
37. When companies like Defendant build their websites, they install or integrate various third-party scripts into the code of the website to collect data from users or perform other functions.[4]

[4] See *Third-party Tracking*, PIWIK, https://piwik.pro/glossary/third-party-tracking/ ("Third-party tracking refers to the practice by which a tracker, other than the website directly visited by

38. Oftentimes, third-party scripts are installed on websites "for advertising purposes."[5] Further, "[i]f the same third-party tracker is present on many sites, it can build a more complete profile of the user over time."

39. To make Defendant's Website load on a user's internet browser, the browser sends an "HTTP request" or "GET" request to Defendant's server where the relevant Website data is stored. In response to the request, Defendant's server sends an "HTTP response" back to the browser with a set of instructions. A general diagram of this process is pictured at Figure 1, which explains how Defendant's Website transmits instructions back to users' browsers in response to HTTP requests. (See Figure 1.)

Figure 1:



40. The server's instructions include how to properly display the Website—*e.g.*, what images to load, what text should appear, or what videos should play.

41. When a user navigates to a webpage (by entering a URL address directly or clicking a hyperlink containing the address), that user's browser contacts the DNS (Domain

---

the user, traces or assists in tracking the user's visit to the site. Third-party trackers are snippets of code that are present on multiple websites. They collect and send information about a user's browsing history to other companies…").

[5] *Id.*

Name System) server, which translates the web address of that website into a unique IP (Internet Protocol) address.

42. An IP address is a unique identifier for a device, which is expressed as four sets of numbers separated by periods *(e.g.*, 192.168.123.132). Much like a telephone number, an IP address guides or routes an intentional communication signal (*i.e.*, a data packet) from one device to another. An IP address is essential for identifying a device on the internet or within a local network, facilitating smooth communication between devices.

43. When a user's browser navigates to a webpage, it sends an HTTP request to the server identified by the webpage's IP address. This request is for the specific resource located at the URL. If the server fulfils this request, it issues an HTTP response, which includes the status of the request and, typically, the requested content. This content is then transmitted in small chunks, known as data packets, and reassembled into the complete webpage upon arrival by the user's browser.[6]

44. This request URL includes a domain name and path, which identify the specific content being accessed on a website and its location within the website's structure.

45. The request URL typically contains parameters. Parameters are values added to a URL to transmit data to the recipient, prefaced by a question mark to signal the use of parameters. Parameters direct a web server to provide additional context-sensitive services. (See

Figure 2:

[6] *What is an IP Address – Definition and Explanation*, KASPERSKY, https://usa.kaspersky.com/resource center/definitions/what-is-an-ip-address (last accessed January 30, 2025).

Figure 2.)

46. Defendant has implemented a myriad of sophisticated tracking tools that operate covertly when users access and navigate its Website, including Facebook, TikTok, and Taboola. The Tracking Parties use a myriad of cookies and other persistent trackers (collectively, the "Tracking Tools") to capture a user's IP address and long-string URLs revealing a host of information about that user's private activities on the Website, as explained at greater depth below.

B. The Facebook Tracking Pixel

47. Facebook is the largest social networking site on the planet, touting 2.9 billion monthly active users.[7] Facebook describes itself as a "real identity platform,"[8] meaning users are allowed only one account and must share "the name they go by in everyday life."[9] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[10]

48. Facebook generates revenue by selling advertising space on its website.[11]

49. Facebook sells advertising space by highlighting its ability to target users.[12] Facebook can target users so effectively because it surveils user activity both on and off its site.[13]

---

[7] Sean Burch, *Facebook Climbs to 2.9 Billion Users, Report 29.1 Billion in Q2 Sales*, YAHOO (July 28, 2021), https://www.yahoo.com/now/facebook-climbs-2-9-billion-202044267.
[8] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).
[9] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.
[10] FACEBOOK, SIGN UP, https://www.facebook.com/
[11] Mike Isaac, *Facebook's profit surges 101 percent on strong ad sales*., N.Y. TIMES (July 28, 2021), https://www.nytimes.com/2021/07/28/business/facebook-q2-earnings.html.
[12] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706.
[13] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[14] Facebook compiles this information into a generalized dataset called "Core Audiences," which businesses use to apply highly specific filters and parameters for their targeted advertisements.[15]

50. Businesses that advertise can also build "Custom Audiences."[16] Custom Audiences enable businesses to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[17] Businesses can use a Custom Audience to target existing customers directly, or they can use it to build a "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[18] Unlike Core Audiences, Custom Audiences require an advertiser to supply the underlying data to Facebook. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools," which collect and transmit the data automatically.[19] One such Business Tool is the Facebook Tracking Pixel.

---

[14] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.
[15] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.
[16] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.
[17] FACEBOOK, ABOUT EVENTS CUSTOM AUDIENCE, https://www.facebook.com/business/help/366151833804507?id=300360584271273.
[18] FACEBOOK, ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328.
[19] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.

51. The Facebook Tracking Pixel is a piece of code that businesses, like Defendant, can integrate into their website. Once activated, the Facebook Tracking Pixel "tracks the people and type of actions they take."[20] When the Facebook Tracking Pixel captures an action, it sends a record to Facebook. Once this record is received, Facebook processes it, analyzes it, and assimilates it into datasets like the Core Audiences and Custom Audiences.

52. Businesses control what actions—or, as Facebook calls it, "events"—the Facebook Tracking Pixel will collect, including the website's metadata, along with what pages a visitor views.[21] Business can also configure the Facebook Tracking Pixel to track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[22] A business can also create their own tracking parameters by building a "custom event."[23]

53. Businesses control how the Facebook Tracking Pixel identifies visitors. The Facebook Tracking Pixel is configured to automatically collect "HTTP Headers" and "Pixel-specific Data."[24] HTTP Headers collect "IP addresses, information about the web browser, page location, document, referrer and persons using the website."[25] Pixel-specific Data includes "the Pixel ID and cookie."[26]

---

[20] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.
[21] *See* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; see also FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142.
[22] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.
[23] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142.
[24] FACEBOOK, FACEBOOK PIXEL, https://developers.facebook.com/docs/facebook-pixel/.
[25] *Id.*
[26] *Id.*

54. The Facebook Tracking Pixel also allows advertisers "to track [its] website visitors' actions," which Meta calls conversion tracking.[27] "Tracked conversions … can be used to analyze [Defendant's] return on ad investment."[28] Notably, "[e]ach time the Pixel loads, it automatically … track[s]" and records the URL that a website user viewed.[29] In other words, so long as an advertised has installed the Facebook Tracking Pixel on the their website, anyone who views that webpage—meaning all website users—"will be tracked using that" automatic URL tracker.[30] And, as mentioned above, the tracked URL discloses to Facebook the exact video(s) that a website user views. Indeed, Facebook even warns advertisers to "make sure" the website URLs are specific enough so advertisers "can define visitor actions exclusively based on unique … website URLs."[31]

55. "Once tracked, custom conversions"—such as the URL tracking tool— "can be used to optimize [] ad campaigns"[32] through other Facebook tools such as Ads Insights.[33] Notably, this part of Facebook's functionality ignores users' decision to opt out of tracking, collecting the same data it would otherwise through "a connection between an advertiser's server and Meta's Conversion API endpoint."[34]

56. After receiving information from businesses like Defendant, Facebook processes

---

[27] FACEBOOK, CONVERSION TRACKING, https://developers.facebook.com/docs/meta-pixel/
implementation/conversion-tracking.
[28] *Id*.
[29] FACEBOOK, CUSTOM CONVERSIONS,, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking#custom-conversions.
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] FACEBOOK, CUSTOM CONVERSIONS INSIGHTS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking#custom-conversions.
[34] *Id.*

it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

57. Facebook confirms, in its "Meta Business Tools Terms,"[35] that it has the capability to use the information it collects for purposes other than recording it and conveying it to advertisers. For instance, Facebook can use the information it collects "to promote safety and security on and off the Meta Products, for research and development purposes and to maintain the integrity of and to provide and improve the Meta Products."[36] In other words, Facebook can use the wiretapped information for its own "research and development," and to "protect" its own products and services.[37]

58. Facebook can also connect all information it collects to analyze and generate reports regarding advertising campaigns, create custom audience sets that can be shared with other advertisers, and "use your Event Data for ads delivery only after aggregating such Event Data with other data collected from other advertisers or otherwise collected on Meta Products."[38]

59. Further, Facebook can use the event data to help websites "reach people with transactional and other commercial messages on [Facebook] Messenger and other Meta Products."[39]

60. At all relevant times herein, Defendant's Website hosts and/or has hosted the Facebook Tracking Pixel and other Facebook tracking tools—including the URL trackers—described above.

61. More specifically, the Facebook Pixel that Defendant installed and used tracked,

---

[35] FACEBOOK, META BUSINESS TOOLS TERMS, https://m.facebook.com/legal/businesstech.
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*

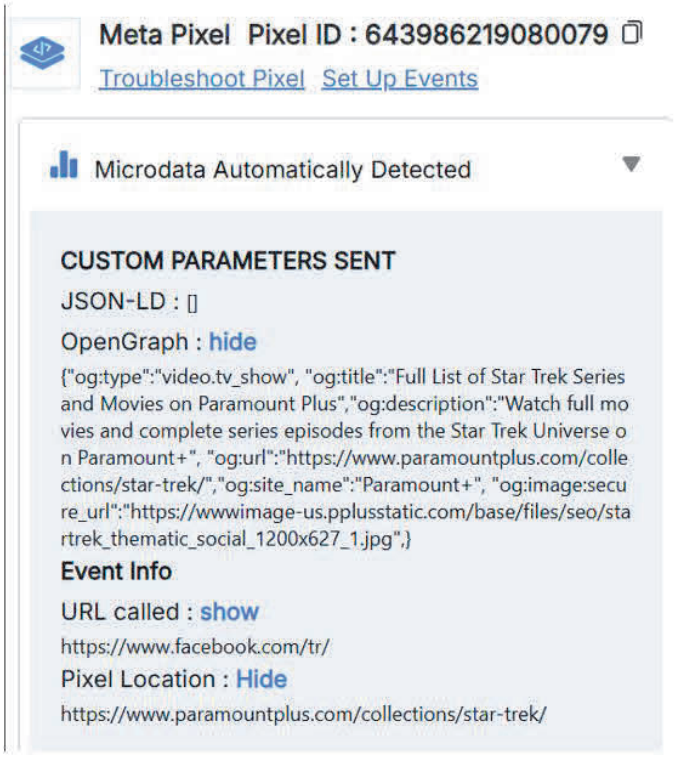
recorded, and sent Facebook its subscribers' granular Website and apps activity, including the names of specific videos that subscribers requested and/or viewed each time through Defendant's Website and apps. The information is not merely metadata.

62. Defendant's motivation for using the Facebook Tracking Pixel and related Facebook Business Tools is simple—it financially benefits Defendant in the form of advertising and information services that Defendant would otherwise have to pay for.

63. The information Facebook receives from Defendant identifies subscribers based on their unique and persistent Facebook IDs ("FID"), which is sent to Facebook as one data point alongside the title of the video content the specific subscriber requested or viewed. Defendant's use of the Facebook Tracking Pixel is depicted below. The term "PageView" discloses a video's URL whenever a viewer accesses that webpage.

Figure 1:

Figure 2:



64. Defendant's use of the Facebook Tracking Pixel permits an ordinary person to identify a video's content, title, and URL.

65. When a visitor watches a video on the Website while logged into Facebook, Defendant compels a visitor's browser to transmit the c_user cookie to Facebook. The c_user cookie contains that visitor's unencrypted Facebook ID. When accessing the above video, for example, Defendant compelled the browser to send ten cookies:

Figure 3:

_fbp	fb.1.1735917617339.404575985772091182	.paramountplus.com
c_user	100069197062755	.facebook.com
datr	MBp_ZoLHpSrxxtFYf1rPLJth	.facebook.com
dpr	1.5	.facebook.com
fr	14BgYNERtKTEryrVc.AWWGxcRKsBnsP9oYut7nY2h...	.facebook.com
presence	C%7B%22t3%22%3A%5B%5D%2C%22utc3%22%3...	.facebook.com
ps_l	1	.facebook.com
ps_n	1	.facebook.com
sb	j49zX9S4REMRfpHh77IfeUjk	.facebook.com
wd	1691x830	.facebook.com
xs	22%3Aekbphbv W8f9YxA%3A2%3A1734967094%3...	.facebook.com

66. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.[40] The _fbp cookie contains, at least, an unencrypted value that uniquely identifies a browser.[41] The datr cookies also identifies a browser.[42] Facebook, at a minimum, uses the fr and _fbp cookies to identify users.[43]

67. Without a corresponding Facebook ID, the fr cookie contains, at least, an abbreviated and encrypted value that identifies the browser. The _fbp cookie contains, at least, an unencrypted value that uniquely identifies a browser. Facebook uses both for targeted advertising.

68. The fr cookie will expire after 90 days unless the visitor's browser logs back into

[40] DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.
[41] FACEBOOK, CONVERSION API, https://developers.facebook.com/docs/marketing api/conversions-api/parameters/fbp-and-fbc/.
[42] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/.
[43] *Id.*

Facebook.[44] If that happens, the time resets, and another 90 days begins to accrue.[45]

69. The _fbp cookie will expire after 90 days unless the visitor's browser accesses the same website.[46] If that happens, the time resets, and another 90 days begins to accrue.[47]

70. The Facebook Tracking Pixel uses both first- and third-party cookies. A first party cookie is "created by the website the user is visiting"—*i.e.*, Paramount.[48] A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"— *i.e.*, Facebook.[49] The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

71. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link to Facebook IDs and corresponding Facebook profiles.

72. A Facebook ID is personally identifiable information. Anyone can identify a Facebook profile—and all personal information publicly listed on that profile—by appending the Facebook ID to the end of Facebook.com.

73. Through the Facebook Tracking Pixel's code, these cookies combine the identifiers with the event data, allowing Facebook to know, among other things, what Paramount videos a user has watched.[50]

74. Defendant also chose to use "Automatic Advanced Matching." When activated,

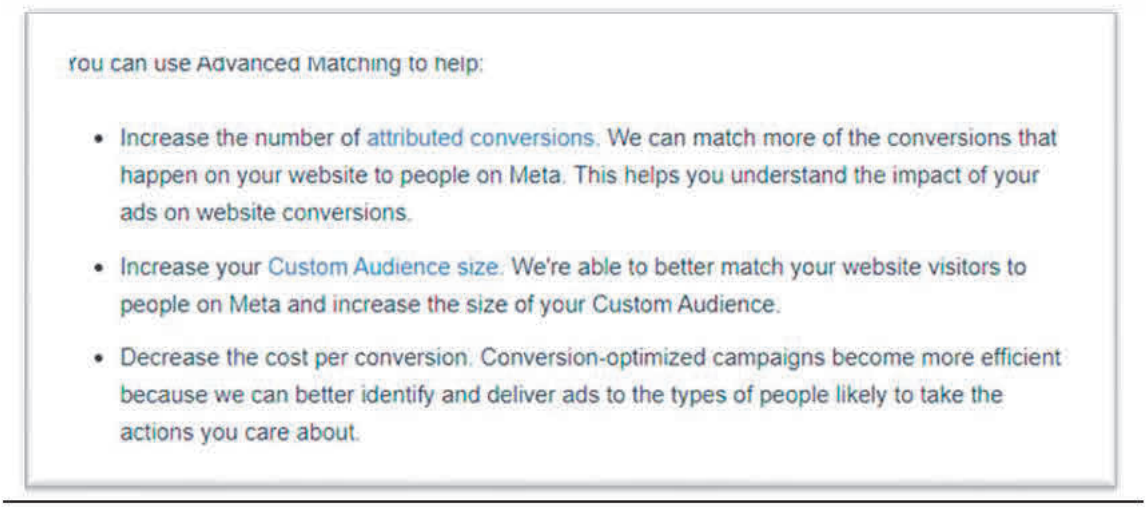
---

[44] *Id.*
[45] Confirmable through developer tools.
[46] *Id.*
[47] Also confirmable through developer tools.
[48] PC MAG, *FIRST-PARTY COOKIES*, https://www.pcmag.com/encyclopedia/term/first-party cookie. This is confirmable by using developer tools to inspect a website's cookies and track network activity.
[49] *Id.*
[50] *Id.*

the Facebook Tracking Pixel "look[s] for recognizable form field and other sources on your website that contain information such as first name, last name and email."[51] The Facebook Tracking Pixel's code collect[s] that information, "along with the event, or action, that took place."[52] This information is "hashed,"[53] meaning it is "[a] computed summary of digital data that is a one-way process."[54] In other words, it "cannot be reversed back into the original data."[55]

75. Paramount discloses this information so it can better match visitors to their Facebook profiles, which thereby allows Paramount to better track analytics and target its advertisements:

Figure 4:



76. Paramount's Facebook Tracking Pixel is configured to scan form fields

[51] FACEBOOK, GET STARTED, https://developers.facebook.com/docs/meta-pixel/get-started.
38 https://www.facebook.com/business/help/611774685654668?id=1205376682832142
[52] FACEBOOK, ABOUT ADVANCED MATCHING FOR WEB, https://www.facebook.com/business/help/611774685654668?id=1205376682832142.
[53] DEFINITION OF HASH, https://www.pcmag.com/encyclopedia/term/hash
[54] *Id.*
[55] *Id.*

containing a user's email, first name, last name, gender, phone number, city, state, and zip code:[56]

Figure 5:

```
f.ensureModuleRegistered("SignalsPixelPIIConstants", function() {
    return function(g, h, i, j) {
        var k = {
            exports: {}
        };
        k.exports;
        (function() {
            "use strict";
            var a = f.getFbeventsModules("SignalsFBEventsUtils")
              , b = a.keys;
            a = a.map;
            var c = {
                ct: "ct",
                city: "ct",
                dob: "db",
                dobd: "dobd",
                dobm: "dobm",
                doby: "doby",
                email: "em",
                fn: "fn",
                f_name: "fn",
                gen: "ge",
                ln: "ln",
                l_name: "ln",
                phone: "ph",
                st: "st",
                state: "st",
                zip: "zp",
                zip_code: "zp"
```

77. Paramount knows Facebook will match the Advanced Matching parameters with a subscriber's subsequent activity, thereby helping Paramount "[i]ncrease the number of attributed conversions," "[i]ncrease [its] Custom Audience size," and "[d]ecrease the cost per

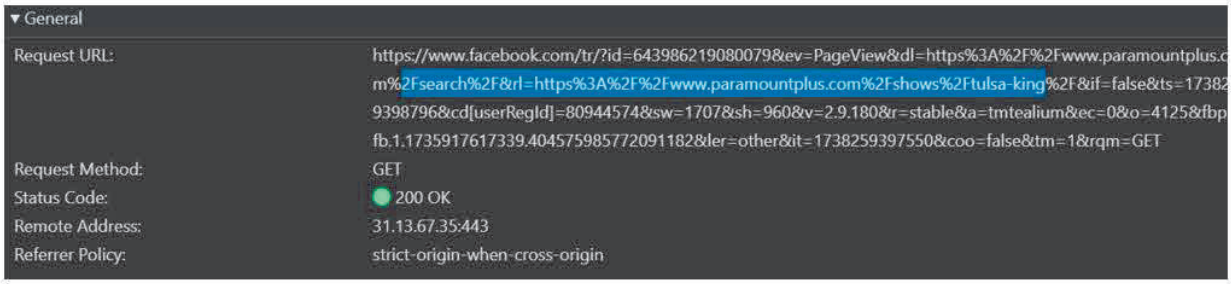
[56] Facebook provides a corresponding look-up table: FACEBOOK, ADVANCED MATCHING, https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching.

conversion."[57]

78. In addition to capturing and sharing its subscribers PII and irrespective of how the they reached the web watching page, through its URL tracking technology, also intercepted and shared button clicks and search terms when subscribers browse videos to watch on the Website.

79. For example, when a subscriber searches for "Tulsa King" on the Website, the Facebook Tracking Pixel captures the search terms and resulting webpage, as depicted blow.

Figure 6:



80. Aside from capturing its subscribers private communications within the Website, capturing and sharing these searches through Facebook's URL trackers also discloses their video watching history.

81. Facebook confirms that it matches activity on Paramount with a user's profile. Facebook allows users to download their "off-site activity," which is a "summary of activity that businesses and organizations share with us about your interactions, such as visiting their apps or websites."[58] Here, the off-site activity report confirms Paramount identifies an individual's video

[57] FACEBOOK, ABOUT ADVANCED MATCHING FOR WEB, https://www.facebook.com/business/help/611774685654668?id=1205376682832142.
[58] FACEBOOK, WHAT IS OFF-FACEBOOK ACTIVITY?, https://www.facebook.com/help/2207256696182627. As discussed there, the Off-Facebook Activity is only a "summary" and Facebook acknowledges "receiv[ing] more details and activity than what appears in your Facebook activity." What is more, it omits "information we've received when you're not logged int Facebook, or when we can't confirm that you've previously used Facebook on that device."

viewing activities:

Figure 7:

82. The "ID" shown here is the same Facebook Pixel ID visible in the first 1, *supra*. The Facebook Pixel ID is a numerical code that uniquely identifies each Pixel.[59] In practice, this means Paramount's Facebook Tracking Pixel has a Pixel ID that differs from all other websites. All subscribers who view videos on Defendant's Website can pull their off-site activity report and see the same Pixel ID.

C. TikTok

83. At all relevant times herein, Defendant's Website hosts and/or has hosted TikTok's trackers on its Website and apps. TikTok, owned by Chinese parent company ByteDance Ltd., launched in 2017 and is headquartered in both Los Angeles, CA and Singapore. TikTok represents that it is "the leading destination for short-form mobile video[.]"[60] The company's app has over one billion users and monetizes its data for advertising purposes—its main source of revenue.[61] Last year, TikTok's revenue totaled $16 billion in the United States

[59] FACEBOOK, GET STARTED, https://developers.facebook.com/docs/meta-pixel/get-started.
[60] *About TikTok*, TIKTOK, https://www.tiktok.com/about?lang=en (last visited Oct. 31, 2024).
[61] Mansoor Iqbal, *TikTok Revenue and Usage Statistics (2024)*, BUSINESS OF APPS (July 8, 2024), https://www.businessofapps.com/data/tik-tok-statistics/; see also NewFronts '24: Introducing New Premium Ad Solutions for Marketers, TIKTOK COMMUNITY (May 2, 2024), https://newsroom.tiktok.com/en-us/newfronts-24-introducing-new-premium-ad-solutions-for marketers; Zheping Huang, *TikTok Has a Few Main Ingredients for Making Money*,

alone.[62]

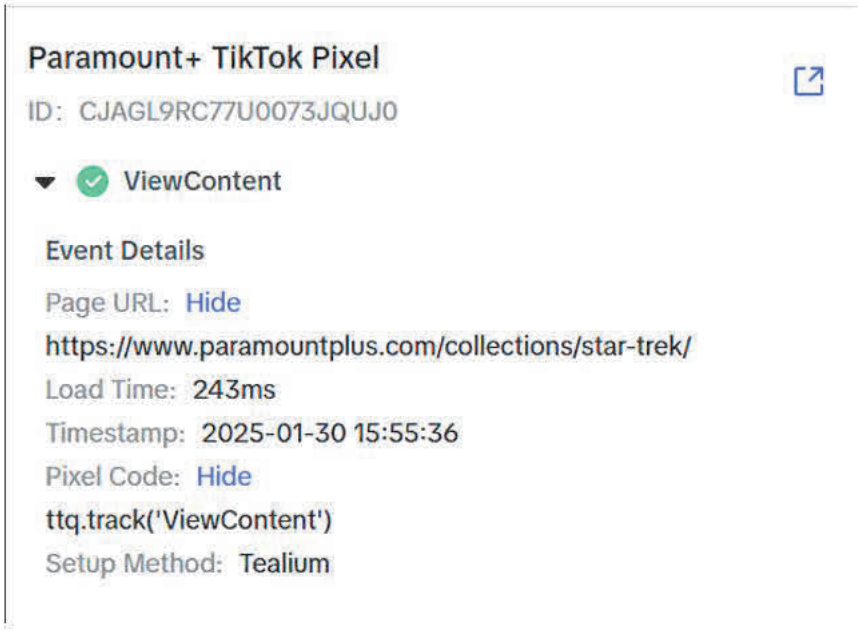
84. In addition to its social media offerings, TikTok develops several analytics tools for use by web and app developers. TikTok allows web and app developers to incorporate its analytics tools into their platforms free of charge for the purposes of gaining customer insights, measuring customer interactions, and optimizing marketing performance. In exchange for the free use of its tools, TikTok automatically receives user data associated with its embedded business tools. Like Facebook, the information TikTok receives from Defendant identifies consumers based on their unique and persistent TikTok identifiers, which is sent to TikTok as one data point alongside the title of the video content the specific subscriber requested or viewed. Defendant's use of the Facebook Tracking Pixel is depicted below. The term "ViewContent" discloses a video's URL whenever a viewer accesses that webpage.

[Intentionally Left Blank]

BLOOMBERG (June 28, 2022), https://www.bloomberg.com/news/newsletters/2022-06-28/how-does-tiktok make-money-app-relies-on-a-few-main-ingredients.

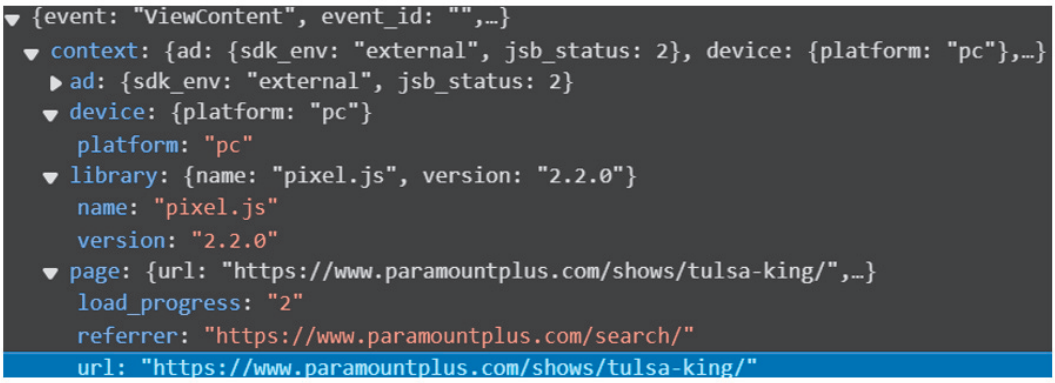
[62] *TikTok's US Revenue Hits $16 bln as Washington Threatens Ban, FT Reports*, REUTERS (Mar. 15, 2024), https://www.reuters.com/technology/tiktoks-us-revenue-hits-16-bln-washington-threatens-ban-ft-reports-2024-03-15/ (last visited Oct. 31, 2024).

Figure 1:



85. In addition to capturing and sharing its consumer's PII and irrespective of how the they reached the web watching page, TikTok also uses URL tracking technology, to intercept and shared button clicks and search terms when subscribers browse videos to watch on the Website.

Figure 2:



86. Paramount's TikTok Tracking Pixel is configured to scan form fields containing a user's email, first name, last name, phone number, city, state, country, and zip code:

Figure 3:

87. In addition, when a user accesses the Website, Defendant compels their browser to send 46 persistent cookies to TikTok.

Figure 4:

_fbp	fb.1.1738251290786.2128641224	.tiktok.com
_ga	GA1.1.1480947894.1738251289	.tiktok.com
_ga_HV1FL86553	GS1.1.1738251288.1.1.1738251581.0.0.1943149790	.tiktok.com
_ga_Y2RSHPPW88	GS1.1.1738251288.1.1.1738251581.0.0.623159323	.tiktok.com
_tt_enable_cookie	1	.tiktok.com
_ttp	2sM3TAXSCte99WRSHPodrspwNKA	.tiktok.com
ac_csrftoken	f440d2055fab4b99abc5e8bec3741e0b	.tiktok.com
cmpl_token	AgQQAPNSF-RO0rPsSKBhNJ0T_Sxi2Drz_6zZYNtjOw	.tiktok.com
d_ticket	889b17538a519e2f5afca77df10d10da74de2	.tiktok.com
msToken	kdwDOG840b74C65Uidy941MgGOeyvM_XOcVgYLH0kXK...	.tiktok.com
multi_sids	7192994107768587306%3Aff823963b65e3466b1fdeeec6...	.tiktok.com
odin_tt	732327e6bb80465b500c7503b90d66ba442116ef6508c5b...	.tiktok.com
part	stable	.tiktok.com
passport_csrf_token	2585297577d7310f7a8e9b41bf1b29f7	.tiktok.com
passport_csrf_token_d...	2585297577d7310f7a8e9b41bf1b29f7	.tiktok.com
pre_country	US	.tiktok.com
sessionid	ff823963b65e3466b1fdeeec6863c9fb	.tiktok.com
sessionid_ads	754a0349ec460ac00e8386a4f6001db6	.tiktok.com
sessionid_ss	ff823963b65e3466b1fdeeec6863c9fb	.tiktok.com
sessionid_ss_ads	754a0349ec460ac00e8386a4f6001db6	.tiktok.com
sid_guard	ff823963b65e3466b1fdeeec6863c9fb%7C1734018218%7...	.tiktok.com
sid_guard_ads	754a0349ec460ac00e8386a4f6001db6%7C1738251415%...	.tiktok.com
sid_tt	ff823963b65e3466b1fdeeec6863c9fb	.tiktok.com
sid_tt_ads	754a0349ec460ac00e8386a4f6001db6	.tiktok.com
sid_ucp_sso_v1_ads	1.0.0-KDRiMTc4NDFhMzI3MTc4ZTcyMGYzMTJjNDFhYTUw...	.tiktok.com
sid_ucp_v1	1.0.0-KGJjZTNjNDdlYmQ0ZjdlZWQ0NTk5NDU1YjQ2NTUz...	.tiktok.com
sid_ucp_v1_ads	1.0.0-KDZkZmQ0MzlkODE1YTFhYmUwOGYxZDQzOTVjMz...	.tiktok.com
ssid_ucp_sso_v1_ads	1.0.0-KDRiMTc4NDFhMzI3MTc4ZTcyMGYzMTJjNDFhYTUw...	.tiktok.com
ssid_ucp_v1	1.0.0-KGJjZTNjNDdlYmQ0ZjdlZWQ0NTk5NDU1YjQ2NTUz...	.tiktok.com
ssid_ucp_v1_ads	1.0.0-KDZkZmQ0MzlkODE1YTFhYmUwOGYxZDQzOTVjMz...	.tiktok.com
sso_uid_tt_ads	7b150b3cc5b6e46647d5917b2e72298155a6e5fee1e27afd...	.tiktok.com
sso_uid_tt_ss_ads	7b150b3cc5b6e46647d5917b2e72298155a6e5fee1e27afd...	.tiktok.com
sso_user_ads	c9f84da1bbc5fb988b3cc0920407d640	.tiktok.com
sso_user_ss_ads	c9f84da1bbc5fb988b3cc0920407d640	.tiktok.com
store-country-code	us	.tiktok.com
store-country-code-src	uid	.tiktok.com
store-idc	useast5	.tiktok.com
tt-target-idc	useast8	.tiktok.com
tt-target-idc-sign	Z2K9ZW-p8SSs9nGIWp4-Zvhtaobvnng0AbzJSLzRgs9Ncc...	.tiktok.com
tt_chain_token	pPQagS7xDWssXsMuUoDm6A==	.tiktok.com
tta_attr_id_mirror	0.1730405527.7432035149233012753	.tiktok.com
ttwid	1%7Cu9J--sLpVvTCBuDme5ES_Zd6t9Y9RPG_qHRfFhlHLO...	.tiktok.com
uid_tt	45e39ccd5d2a3a3bbde1d2c48e4d28f4fd303afebc73fa5f3...	.tiktok.com
uid_tt_ads	f5b341ccd69f1646df305ff735184d03e470a9789f0c45b1a...	.tiktok.com
uid_tt_ss	45e39ccd5d2a3a3bbde1d2c48e4d28f4fd303afebc73fa5f3...	.tiktok.com
uid_tt_ss_ads	f5b341ccd69f1646df305ff735184d03e470a9789f0c45b1a...	.tiktok.com

88. Although the exact nature and arrangement of Defendant's arrangement with TikTok is unknown at this time given TikTok's covert operations, upon information and belief, Defendant shares enough information to permit an ordinary person, or at minimum TikTok, to identify the video's content, title, and URLs of its subscribers, irrespective of whether they have or are logged into a TikTok account.

D. Taboola

89. At all relevant times herein, Defendant's Website hosts and/or has hosted Taboola's trackers on its Website and apps. Taboola's software is owned by Taboola Inc., a company which leverages data analytics to align digital content with user preferences across its network of publisher websites. As a content recommendation platform, Taboola's trackers are designed to collect user data to optimize content suggestions, enhancing both user experience and content monetization for publishers.

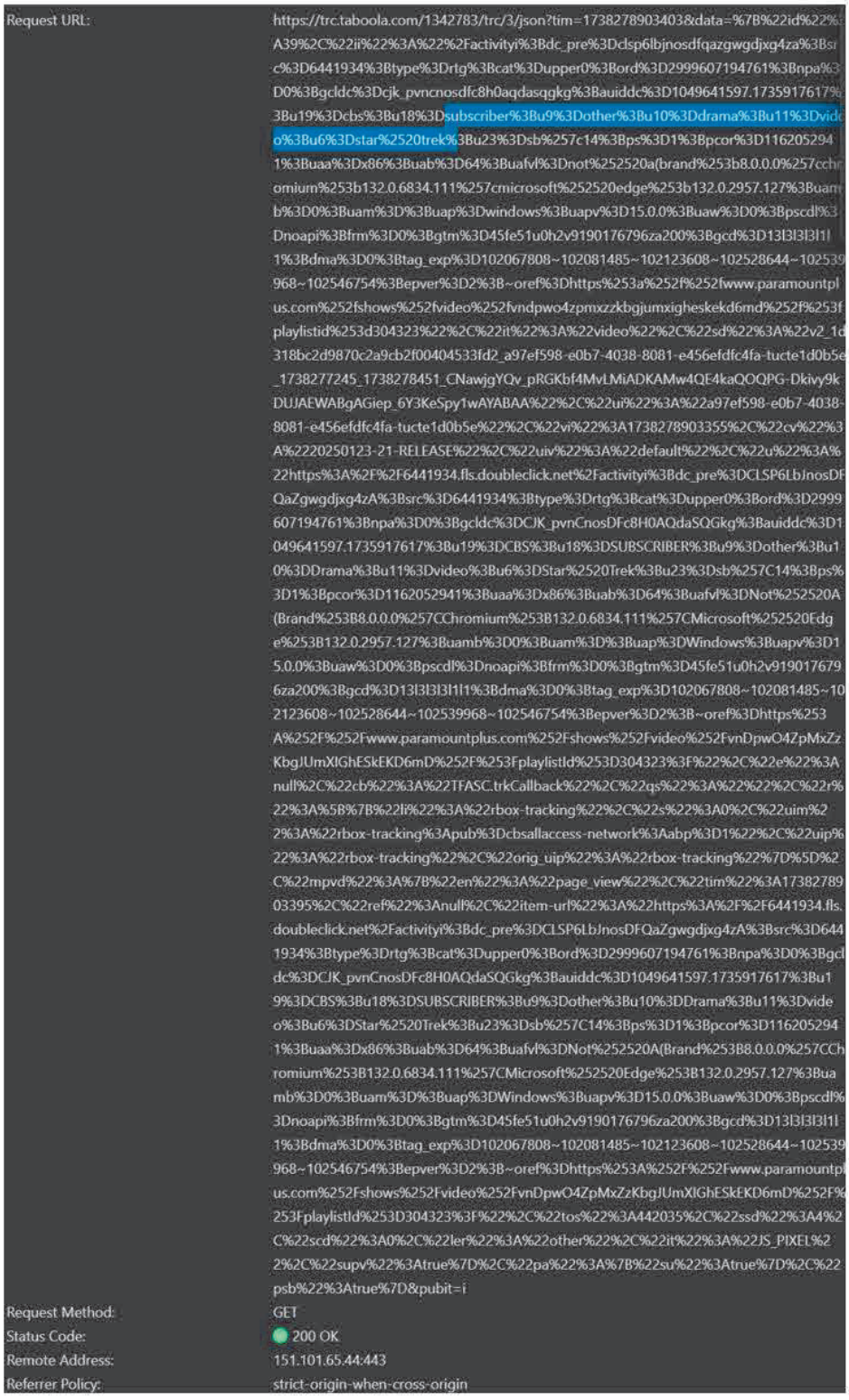
90. When a subscriber first accesses and enters Defendant's Website, the user's browser sends an HTTP request to Defendant's Website server. In turn, Defendant's Website server sends an HTTP response with directions to load the webpage content and to install the Taboola trackers on the user's browser. The Taboola trackers store a website cookie in the user's browser cache and uses that third-party tracker cookie to collect and share that user's IP address with Taboola every time they interact with the Website. (See Figures 1 and 2, identifying Taboola, a long-string URL including the path and parameters revealing extensive information, and the user's IP address (38.108.xx.x)).

///
///
///
///
///

Figure 1:

[Intentionally Left Blank]

Figure 2:


Request URL:
https://trc.taboola.com/1342783/trc/3/json?tim=1738278903403&data=%7B%22id%22%3A39%2C%22ii%22%3A%22%2Factivityi%3Bdc_pre%3Dclsp6lbjnosdfqazgwgdjxg4za%3Bsrc%3D6441934%3Btype%3Drtg%3Bcat%3Dupper0%3Bord%3D2999607194761%3Bnpa%3D0%3Bgcldc%3Dcjk_pvncnosdfc8h0aqdasqgkg%3Bauiddc%3D1049641597.1735917617%3Bu19%3Dcbs%3Bu18%3Dsubscriber%3Bu9%3Dother%3Bu10%3Ddrama%3Bu11%3Dvideo%3Bu6%3Dstar%2520trek%3Bu23%3Dsb%257c14%3Bps%3D1%3Bpcor%3D1162052941%3Buaa%3Dx86%3Buab%3D64%3Buafvl%3Dnot%252520a(brand%253b8.0.0.0%257cchromium%253b132.0.6834.111%257cmicrosoft%252520edge%253b132.0.2957.127%3Buamb%3D0%3Buam%3D%3Buap%3Dwindows%3Buapv%3D15.0.0%3Buaw%3D0%3Bpscdl%3Dnoapi%3Bfrm%3D0%3Bgtm%3D45fe51u0h2v9190176796za200%3Bgcd%3D13l3l3l3l1l1%3Bdma%3D0%3Btag_exp%3D102067808~102081485~102123608~102528644~102539968~102546754%3Bepver%3D2%3B~oref%3Dhttps%253a%252f%252fwww.paramountplus.com%252fshows%252fvideo%252fvndpwo4zpmxzzkbgjumxigheskekd6md%252f%253fplaylistid%253d304323%22%2C%22it%22%3A%22video%22%2C%22sd%22%3A%22v2_1d318bc2d9870c2a9cb2f00404533fd2_a97ef598-e0b7-4038-8081-e456efdfc4fa-tucte1d0b5e_1738277245_1738278451_CNawjgYQv_pRGKbf4MvLMiADKAMw4QE4kaQOQPG-Dkivy9kDUJAEWABgAGiep_6Y3KeSpy1wAYABAA%22%2C%22ui%22%3A%22a97ef598-e0b7-4038-8081-e456efdfc4fa-tucte1d0b5e%22%2C%22vi%22%3A1738278903355%2C%22cv%22%3A%2220250123-21-RELEASE%22%2C%22uiv%22%3A%22default%22%2C%22u%22%3A%22https%3A%2F%2F6441934.fls.doubleclick.net%2Factivityi%3Bdc_pre%3DCLSP6LbJnosDFQaZgwgdjxg4zA%3Bsrc%3D6441934%3Btype%3Drtg%3Bcat%3Dupper0%3Bord%3D2999607194761%3Bnpa%3D0%3Bgcldc%3DCJK_pvnCnosDFc8H0AQdaSQGkg%3Bauiddc%3D1049641597.1735917617%3Bu19%3DCBS%3Bu18%3DSUBSCRIBER%3Bu9%3Dother%3Bu10%3DDrama%3Bu11%3Dvideo%3Bu6%3DStar%2520Trek%3Bu23%3Dsb%257C14%3Bps%3D1%3Bpcor%3D1162052941%3Buaa%3Dx86%3Buab%3D64%3Buafvl%3DNot%252520A(Brand%253B8.0.0.0%257CChromium%253B132.0.6834.111%257CMicrosoft%252520Edge%253B132.0.2957.127%3Buamb%3D0%3Buam%3D%3Buap%3DWindows%3Buapv%3D15.0.0%3Buaw%3D0%3Bpscdl%3Dnoapi%3Bfrm%3D0%3Bgtm%3D45fe51u0h2v9190176796za200%3Bgcd%3D13l3l3l3l1l1%3Bdma%3D0%3Btag_exp%3D102067808~102081485~102123608~102528644~102539968~102546754%3Bepver%3D2%3B~oref%3Dhttps%253A%252F%252Fwww.paramountplus.com%252Fshows%252Fvideo%252FvnDpwO4ZpMxZzKbgJUmXIGhESkEKD6mD%252F%253Fplaylistid%253D304323%3F%22%2C%22e%22%3Anull%2C%22cb%22%3A%22TFASC.trkCallback%22%2C%22qs%22%3A%22%22%2C%22r%22%3A%5B%7B%22li%22%3A%22rbox-tracking%22%2C%22s%22%3A0%2C%22uim%22%3A%22rbox-tracking%3Apub%3Dcbsallaccess-network%3Aabp%3D1%22%2C%22uip%22%3A%22rbox-tracking%22%2C%22orig_uip%22%3A%22rbox-tracking%22%7D%5D%2C%22mpvd%22%3A%7B%22en%22%3A%22page_view%22%2C%22tim%22%3A1738278903395%2C%22ref%22%3Anull%2C%22item-url%22%3A%22https%3A%2F%2F6441934.fls.doubleclick.net%2Factivityi%3Bdc_pre%3DCLSP6LbJnosDFQaZgwgdjxg4zA%3Bsrc%3D6441934%3Btype%3Drtg%3Bcat%3Dupper0%3Bord%3D2999607194761%3Bnpa%3D0%3Bgcldc%3DCJK_pvnCnosDFc8H0AQdaSQGkg%3Bauiddc%3D1049641597.1735917617%3Bu19%3DCBS%3Bu18%3DSUBSCRIBER%3Bu9%3Dother%3Bu10%3DDrama%3Bu11%3Dvideo%3Bu6%3DStar%2520Trek%3Bu23%3Dsb%257C14%3Bps%3D1%3Bpcor%3D1162052941%3Buaa%3Dx86%3Buab%3D64%3Buafvl%3DNot%252520A(Brand%253B8.0.0.0%257CChromium%253B132.0.6834.111%257CMicrosoft%252520Edge%253B132.0.2957.127%3Buamb%3D0%3Buam%3D%3Buap%3DWindows%3Buapv%3D15.0.0%3Buaw%3D0%3Bpscdl%3Dnoapi%3Bfrm%3D0%3Bgtm%3D45fe51u0h2v9190176796za200%3Bgcd%3D13l3l3l3l1l1%3Bdma%3D0%3Btag_exp%3D102067808~102081485~102123608~102528644~102539968~102546754%3Bepver%3D2%3B~oref%3Dhttps%253A%252F%252Fwww.paramountplus.com%252Fshows%252Fvideo%252FvnDpwO4ZpMxZzKbgJUmXIGhESkEKD6mD%252F%253Fplaylistid%253D304323%3F%22%2C%22tos%22%3A442035%2C%22ssd%22%3A4%2C%22scd%22%3A0%2C%22ler%22%3A%22other%22%2C%22it%22%3A%22JS_PIXEL%22%2C%22supv%22%3Atrue%7D%2C%22pa%22%3A%7B%22su%22%3Atrue%7D%2C%22psb%22%3Atrue%7D&pubit=i
Request Method:
GET
Status Code:
200 OK
Remote Address:
151.101.65.44:443
Referrer Policy:
strict-origin-when-cross-origin

91. This entire process takes place behind the scenes in less than a second. Thus, the Taboola trackers appear the moment a user enters the Website, and they are installed without any further action or consent required of the user.

92. Taboola collects IP addresses to allow it to ascertain a user's location and target that user with advertisements tailored to that specific location. According to its website, Taboola uses its "unique data about people's interests and information consumption to recommend the right content to the right person at the right time."[63] Taboola assists advertisers with targeting their campaigns by location, time, browser type, connection type, audience segments, and more.[64]

93. Further, each time a user revisits the Website, the Taboola tracker identifies that user and sends the stored website cookie, including the user's IP address, back to Taboola. Even if a user clears the cookies from the user's browser, it makes no difference: the next time that user visits the Defendant's Website, Taboola re-installs the tracker cookie, resets the tracking process, and resumes transmission of the user's IP address to Taboola on future visits.

Figure 3:

_hjSessionUser_437790	eyJpZCI6ImYzODFkNTUxLTIyZWQtNTdkNS1iODhjLWU5NGJ...	.taboola.com	/	2026-01-30
receive-cookie-deprecation	1	.taboola.com	/	2026-01-31
t_gid	a97ef598-e0b7-4038-8081-e456efdfc4fa-tucte1d0b5e	.taboola.com	/	2026-01-31
t_pt_gid	a97ef598-e0b7-4038-8081-e456efdfc4fa-tucte1d0b5e	.taboola.com	/	2026-01-31

94. Although the exact nature and arrangement of Defendant's arrangement with Taboola is unknown at this time given Taboola's covert operations, upon information and belief, Defendant shares enough information to permit an ordinary person, or at minimum Taboola, to

[63] TABOOLA, *How Taboola Works, Taboola Help Center*, https://help.taboola.com/hc/en-us/articles/115006597307-How-Taboola-Works.
[64] *Id.*

identify the video's content, title, and URLs of its subscribers.

V. Defendant's Intentionally and Knowingly Discloses its Subscribers PII in Violation of the VPPA and CIPA

95. Pursuant to the systematic process detailed above, Defendant's use of the Trackers violates the VPPA, Wiretap Act, and CIPA.

A. Defendant is a Video Tape Service Provider

96. Defendant provides video streaming services to millions of users through its www.Paramountplus.com (the "Website") and other applications, and its primary business is the delivery of on-demand prerecorded video content.

97. Defendant monetizes this content and its platforms by restricting access to video content, and only individuals who register with Defendant are granted access to its video content.

98. To subscribe to Defendant's services, at a minimum, individuals must create an online account and share their identifying information. To maintain a subscription and access videos past the free trial period, users must pay a monthly or yearly subscription fee.

B. Defendant Knowingly Discloses Consumers' PII To Third Parties

99. When subscribers request or view videos on Defendant's Website and apps, their personal viewing information is transmitted to Facebook, TikTok, Taboola and other unauthorized third parties as a result of the Tracking Tools that Defendant purposely installed and implemented on its Website and apps.

100. Defendant controlled its Website, apps, and all of the tracking technologies that it used to transmit its subscribers' personal viewing information to unauthorized parties. Importantly, neither Facebook, TikTok or Taboola would not have received Plaintiffs' or the Class Members' personal viewing information but for Defendant's decision to install and use

Facebook's Business Tools, including the Facebook Pixel and Conversions API,[65] TikTok Tracking Pixel, and Taboola's trackers (*i.e.,* the Tracking Tools), among other tracking technologies on its Website and apps.

101. Moreover, Defendant controlled which data was tracked, recorded, and transmitted when its subscribers requested or viewed its video content.

102. Defendant's knowledge as to its conduct is evidenced by the fact that: (1) it chose to track its digital subscribers' interactions with the Website and apps, including their requests to view shows or movies; (2) it requested and installed lines of code that achieved this purpose; (3) it obtained the lines of code from Facebook, TikTok, Taboola and other third parties in order to achieve this purpose; and (4) it controlled the information that was tracked, recorded, and transmitted via the Website and the apps.

103. The personal viewing information that Defendant obtained from Plaintiffs and the Class Members through the Tracking Tools is valuable data in the digital advertising-related market for consumer information.

104. At no point did Plaintiffs or the Class Members consent to Defendant's disclosure of their video viewing history to third parties. As such, Defendant deprived Plaintiffs and the Class Members of their privacy rights and control over their personal information.

105. The harms described above are aggravated by Defendant's continued retention and commercial use of Plaintiffs' and the Class Members' personal information, including their private video viewing histories and browsing activities.

[65] Notably, the Facebook Tracking Pixel works in conjunction with its Conversion API tool and, as a result, Defendant transmits one copy of its digital subscribers' viewing information directly from its web server to Meta's web servers. Additional copies of this information are also communicated through the use of cookies.

TOLLING

106. The statutes of limitations applicable to Plaintiffs' and the Class Members' claims were tolled by Defendant's conduct and Plaintiffs' and the Class Members' delayed discovery of their claims.

107. As alleged above, Plaintiffs and the Class Members did not know and could not have known when they used the Website that Defendant was disclosing their information and communications to third parties. Plaintiffs and the Class Members could not have discovered Defendant's unlawful conduct with reasonable diligence.

108. Defendant secretly incorporated the Tracking Tools into the Website, providing no indication to consumers that their communications would be disclosed to these third parties.

109. Defendant had exclusive and superior knowledge that the Tracking Entities' Tracking Tools incorporated on its Website would disclose consumers' protected and private information and confidential communications, yet failed to disclose that by interacting with the Website, Plaintiffs' and Class Members' PII would be disclosed to third parties.

110. Plaintiffs and the Class Members could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of the Tracking Entities' Tracking Tools is highly technical and there were no disclosures or other indication that would inform a reasonable consumer or Website user that Defendant was disclosing and allowing the interception of such information to these third parties.

111. The earliest that Plaintiffs and the Class and Members could have known about Defendant's conduct was in connection with their investigation and the work done on their behalf in preparation of filing of this Amended Complaint.

CLASS ACTION ALLEGATIONS

112. Plaintiffs bring this action on behalf of themselves and all other similarly situated persons pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), and (b)(3).

113. Specifically, the **Class** is defined as:

> All persons in the United States who, during the maximum period of time permitted by law, logged into Defendant's Website or Apps and viewed prerecorded content using their mobile or computer browsers.

114. Plaintiffs also seek to represent a **California Subclass** defined as:

> All California citizens who, during the maximum period of time permitted by law, logged into Defendant's Website or Apps and viewed prerecorded content using their mobile or computer browsers.

115. The Class and California Subclass shall be collectively referred to as the "Classes," and Members of the Class and Subclass will collectively be referred to as "Class Members," unless it is necessary to differentiate them.

116. The Classes does not include (1) Defendant, its officers, and/or its directors; or (2) the Judge to whom this case is assigned and the Judge's staff.

117. Plaintiffs reserve the right to amend the above class definition and add additional classes and subclasses as appropriate based on investigation, discovery, and the specific theories of liability.

118. ***Community of Interest***: There is a well-defined community of interest among the Class Members, and the disposition of the claims of the Class Members in a single action will provide substantial benefits to all parties and to the Court.

119. ***Numerosity***: While the exact number of the Class Members is unknown to Plaintiffs at this time and can only be determined by appropriate discovery, upon information and belief, the Class Members number in the millions. The Class Members may also be notified

of the pendency of this action by mail and/or publication through the distribution records of Defendant and third-party retailers and vendors.

120. ***Existence and predominance of common questions of law and fact***: Common questions of law and fact exist as to the Class Members and predominate over any questions affecting only individuals of the Classes. These common legal and factual questions include, but are not limited to:

(a) Whether Defendant collected Plaintiffs' and the Class Members' PII;

(b) Whether Defendant unlawfully disclosed and continues to disclose its users' PII, including their video viewing records, in violation of the VPPA;

(c) Whether Defendant unlawfully disclosed and continues to disclose its users' PII, including their video viewing records, in violation of the Wiretap Act;

(d) Whether Defendant unlawfully disclosed and continues to disclose its users' PII, including their video viewing records, in violation of the CIPA;

(e) Whether Defendant's disclosures were committed knowingly;

(f) Whether Defendant disclosed Plaintiffs' and the Class Members' PII without consent and

(g) Whether Plaintiffs and the Class Members are entitled to actual and/or statutory damages for the aforementioned violations and the amount thereof.

121. ***Typicality:*** Plaintiffs' claims are typical of those of the Classes because Plaintiffs, like all members of the Classes, requested and watched videos on Defendant's Website and had his PII collected and disclosed by Defendant to third parties.

122. ***Adequacy***: Plaintiffs will fairly and adequately represent and protect the interests of the Classes as required by Federal Rule of Civil Procedure Rule 23(a)(4). Plaintiffs are

adequate representatives of the Classes because they have no interests which are adverse to the interests of the members of the Classes. Plaintiffs are committed to the vigorous prosecution of this action and, to that end, Plaintiffs have retained skilled and experienced counsel.

123. Moreover, the proposed Classes can be maintained because they satisfy both Rule 23(a) and 23(b)(3) because questions of law or fact common to the Classes predominate over any questions affecting only individual members and a Class Action is superior to all other available methods of the fair and efficient adjudication of the claims asserted in this action under Federal Rule of Civil Procedure 23(b)(3) because:

(a) The expense and burden of individual litigation makes it economically unfeasible for members of the Classes to seek to redress their claims other than through the procedure of a class action;

(b) If separate actions were brought by individual members of the Classes, the resulting duplicity of lawsuits would cause members of the Classes to seek to redress their claims other than through the procedure of a class action; and

(c) Absent a class action, Defendant likely will retain the benefits of its wrongdoing, and there would be a failure of justice.

CAUSES OF ACTION

COUNT I
Violation of the Video Privacy Protection Act
18 U.S.C. § 2710, *et seq.*
(On Behalf of Plaintiffs and the Class)

124. Plaintiffs incorporate by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

125. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally-identifiable information" concerning any "consumer" to a third-party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

126. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials." Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it engaged in the business of renting, selling, and delivering audiovisual materials—including the prerecorded videos that Plaintiffs and the Class Members requested and viewed on the Website and apps—and those deliveries affect interstate or foreign commerce.

127. As defined in 18 U.S.C. § 2710(a)(1), a "consumer" means "any renter, purchaser, or subscriber of goods or services from a video tape service provider." Plaintiffs and the Class Members are "consumers" because they subscribed to Defendant's Website and apps, which provide video content to users. In so doing, Plaintiffs and the Class Members created an account to access Defendant's Website and apps and provided Defendant, at a minimum, their names, emails, addresses, credit card information, and other persistent cookies containing their PII,

including the title of the videos they requested and/or viewed.

128. Defendant knowingly caused Plaintiffs' and the Class Members' personal viewing information, as well as the above-referenced unique identifiers, to be disclosed to third parties, including Facebook, TikTok, and Taboola. This information constitutes "personally identifiable information" under 18 U.S.C. § 2710(a)(3) because it identified each Plaintiffs and Class Members to third parties as individuals who viewed Defendant's video content, including the specific prerecorded video materials requested and/or viewed on the Website and apps. This information allowed third parties, such as Facebook, TikTok, and Taboola to identify each Plaintiffs' and Class Member's specific video viewing preferences and habits.

129. As set forth in 18 U.S.C. § 2710(b)(2)(B), "informed, written consent" must be (1) "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer;" and (2) "at the election of the consumer…is either given at the time the disclosure is sought or is given in advance for a set period of time not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner." Defendant failed to obtain informed, written consent from Plaintiffs and the Class Members under this definition.

130. Defendant was aware that the disclosures to third parties that it shared through the Tracking Tools that it incorporated in its Website and apps identified Plaintiffs and the Class Members. Indeed, both Facebook and TikTok publicly tout their abilities to connect PII to individual user profiles. Defendant also knew that Plaintiffs' and the Class Members' personal viewing information was disclosed to third parties because Defendant programmed the Tracking Tools into the Website's and apps' code so that third parties would receive the video titles and subscriber's unique third-party identifiers when a subscriber requested and/or viewed a prerecorded video on the Website or apps. The purpose of those trackers was to obtain

identifiable analytics and intelligence for Defendant about its user base, while also benefiting Facebook, TikTok, and Taboola, among other third parties, by providing them with additional data that they can leverage for their advertising, analytics and/or other services.

131. Nor were Defendant's disclosures made in the "ordinary course of business" as the term is defined by the VPPA. In particular, the Website's and app's disclosures to Facebook and TikTok were not necessary for "debt collection activities, order fulfillment, request processing, [or] transfer of ownership." 18 U.S.C. § 2710(a)(2).

132. On behalf of themselves and the Class Members, Plaintiffs seeks declaratory relief, statutory damages of $2,500 for each violation of the VPPA pursuant to 18 U.S.C. § 2710(c), and reasonable attorneys' fees and costs.

Count II
Violation of the Federal Wiretap Act
18 U.S.C. § 2710, *et seq.*
(On behalf of Plaintiffs and the Class)

133. Plaintiffs incorporate by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

134. The Federal Wiretap Act prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication. 18 U.S.C. §§ 2510 *et seq.*

135. The Wiretap Act confers a civil private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

136. The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

137. The Wiretap Act defines "contents" as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

138. The Wiretap Act defines "person" as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

139. The Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).

140. Defendant is a person for the purposes of the Wiretap Act.

141. The software deployed by Facebook, TikTok, and Taboola (*i.e.*, the "Tracking Tools") constitute a "device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

142. The confidential communications Plaintiffs and members of the Class had with the Website, in the form of their PII and personal viewing history, were intercepted by Facebook, TikTok, and Taboola (*i.e.*, the "Tracking Entities") and such communications were "electronic communications" under 18 U.S.C. § 2510(12).

143. While the Wiretap Act allows a single party to consent to the interception of an electronic communication, single party consent is only acceptable where the communication is not "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. §2511(2)(d).

144. Plaintiffs and the Class Members had a reasonable expectation of privacy in their electronic communications with the Website in the form of their search terms submitted to the

Website and browsing information, and Defendant's breach of that expectation rises to the level of a common law tort. Furthermore, Plaintiffs the Class Members had a reasonable expectation in the privacy of their electronic communications with the Website, including descriptions and summaries of the videos they watched, searched for, requested, or subscribed to unlock access to, along with their identifying information equivalent to the expectation of privacy codified under the VPPA and CIPA. As such, Defendant's use of the Tracking Tools also constitutes a tortious act under the laws of the United States and California.

145. Plaintiffs and the Class Members reasonably expected that the Tracking Entities were not intercepting, recording, or disclosing their electronic communications with the Website.

146. Within the relevant time period, the electronic communications between Plaintiffs the Class Members and the Website was intercepted by the Tracking Tools the instant they were sent to the Website, without consent, and for the unlawful and wrongful purpose of monetizing their private information, which includes the purpose of using such private information to develop advertising and marketing strategies.

147. Interception of Plaintiffs' and the Class Members' confidential communications with the Website occur whenever a subscriber uses the search bar within the Website, and when navigating various webpages of the Website, including those containing videos.

148. At all relevant times, Defendant's conduct was knowing, willful, and intentional, as Defendant is a sophisticated party with full knowledge regarding the functionality of the Tracking Entities and the functionality of the Tracking Tools, including that allowing the Tracking Tools to be implemented on the Website would cause the private communications of its subscribers to be shared with third parties.

149. Plaintiffs and the Class Members were never asked for their consent to expose

their confidential electronic communications with the Website to third parties. Indeed, such consent could not have been given as the Tracking Entities and Defendant never sought any form of consent from Plaintiffs or the Class Members to intercept, record, and disclose their private communications with the Website.

150. As detailed above, the Tracking Entities' unauthorized interception, disclosure and use of Plaintiffs' and the Class Members' confidential communications was only possible through the Defendant's knowing, willful, or intentional placement of the tracking tools on the Website. 18 U.S. Code § 2511(1)(a).

151. Plaintiffs and members of the Class have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications in violation of 18 U.S.C. § 2520. As such, Plaintiffs and members of the Class are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class Members and any profits made by Defendant as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; (2) appropriate equitable or declaratory relief; and (3) reasonable attorneys' fees and expenses.

Count III
Intrusion Upon Seclusion
(On behalf of Plaintiffs and the California Subclass)

152. Plaintiffs incorporate by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

153. Plaintiffs bring this claim pursuant to California law.

154. To state a claim for intrusion upon seclusion "[Plaintiffs] must possess a legally protected privacy interest … [Plaintiffs'] expectations of privacy must be reasonable … [and Plaintiffs] must show that the intrusion is so serious in 'nature, scope, and actual or potential

impact as to constitute an egregious breach of the social norms.'" *Hernandez v. Hillsides, Inc.* 47 Cal. 4th 272, 286-87 (2009).

155. Plaintiffs and the California Subclass Members maintained a reasonable expectation of privacy in their communications with Defendant via its Website. Users' search terms, browsing history, IP addresses, geolocation data, and website activity have been recognized by society as sensitive information.

156. Courts have recognized that users have a reasonable expectation of privacy in URLs that disclose unique search terms or the particular document within a website that a person views. *Heerde v. Learfield Commc'ns, LLC*,, 2024 WL 3573874 (C.D. Cal. July 19, 2024) (citing *Brown v. Google LLC*, 685 F.Supp.3d 909, 941 (N.D. Cal. 2023)).

157. Plaintiffs and the California Class Members' reasonable expectation of privacy is supported by the VPPA's recognition that PII is sensitive information that must be protected from unauthorized disclosure.

158. Plaintiffs and California Subclass Members have an interest in: (i) precluding the dissemination and/or misuse of their sensitive and confidential information; and (ii) being free to search for and consume audio video materials without observation, intrusion or interference, including, but not limited to, the right to visit and interact with internet websites without being subjected to wiretaps without Plaintiffs and Class Members' knowledge or consent.

159. As explained above, Defendant's actions constitute a serious invasion of privacy that was an egregious breach of social norms, such that the breach was highly offensive to a reasonable person because:

i. The invasion of privacy occurred in a highly sensitive setting – users private consumption of videos provided by Defendant, a video service provider, within

the Website;

ii. Defendant had no legitimate objective or motive in invading Plaintiffs' and Class Members' privacy in such a manner;

iii. Defendant violated multiple laws by invading Plaintiffs and Class Members' privacy, including the VPPA and CIPA;

iv. Defendant deprived Plaintiffs and Class Members of the ability to control dissemination of their personal viewing habits and consumption; and

v. Defendant's action is also unacceptable as a matter of public policy because it undermine the relationship between consumers and their video tape service providers.

160. By creating detailed profiles of Plaintiffs' and the California Subclass Members' activities on the Website to the Tracking Entities—including their video viewing history and URLs divulging their private browsing within the Website—poses a serious risk to their autonomy.

161. For instance, those profiles are and can be used to further invade Plaintiffs' and California Subclass Members' privacy by, for example. allowing third parties to learn intimate details of their video viewing habits and target them for advertising, political, and other purposes, thereby harming them by selling this data to advertisers and potentially data brokers without their consent.

162. Accordingly, Plaintiff and Class and California Subclass Members seek all relief available for invasion of privacy claims under common law.

Count IV
Violation of the California Invasion of Privacy Act

Cal. Penal Code § 631, *et seq.*, ("CIPA")
(On behalf of Plaintiffs and the California Subclass)

163. Plaintiffs incorporate by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

164. Section 631(a) of CIPA provides for damages and other relief against any person who "by means of any machine, instrument, contrivance, or in any other manner," did any of the following:

a. Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;

Or

b. Willfully and without the consent of all parties to the communication,or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;

Or

c. Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained;

Or

d. Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

165. CIPA § 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be

construed broadly to effectuate its remedial purpose of protecting privacy); *see also Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications.").

166. The Facebook, TikTok, and Taboola trackers (*i.e.*, the "Tracking Tools") are each a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

167. Facebook, TikTok, and Taboola (*i.e.*, the "Tracking Entities") are each "separate legal entit[ies] that offer[] [a] 'software-as-a-service' and not merely [] passive device[s]." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, each Tracking Entity had the capability to use the wiretapped information for a purpose other than simply recording the communications and providing the communications to Defendant. Accordingly, the Tracking Entities were each a third party to any communication between Plaintiffs and the California Subclass Members, on the one hand, and Defendant, on the other. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

168. At all relevant times, the Tracking Entities willfully and without the consent of all parties to the communication, and in an unauthorized manner, read, attempted to read, and learned the contents the electronic communications of Plaintiffs and the California Subclass Members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

169. Specifically, the Tracking Entities intercepted and/or read Plaintiffs' and the California's Subclass Members highly detailed URL trackers revealing their:

a. Search queries to find videos on the Website;

b. The path and parameters of the URLs of the webpages which caused navigation to

specific videos within the Website either through their search queries or by virtue of clicking on a link embedded within the Website; and/or

c. Creation of an account and membership subscription within the Website and/or

d. The specific titles of the videos viewed and/or requested within the Website.

170. At all relevant times, Defendant aided, agreed with, employed, or otherwise enabled the Tracking Entities to intercept the electronic consumers of Plaintiffs and California Subclass Members.

171. Plaintiffs and California Subclass Members did not provide their prior consent to the Tracking Entities intentional interception, reading, learning, recording, collection, and usage of Plaintiffs' and the California Subclass Members' electronic communications. Nor did Plaintiffs or the California Subclass Members provide their prior consent to Defendant aiding, agreeing with, employing, or otherwise enabling the same.

172. The wiretapping of Plaintiffs and California Subclass Members occurred in California, where Plaintiffs and the California Subclass Members accessed the Website and apps, and where the Tracking Entities—as enabled by Defendant—routed Plaintiffs and the California Subclass Members' electronic communications to the Tracking Entities respective servers.

173. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and California Subclass Members have been injured by Defendant's violations of CIPA § 631(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

Count V
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 638.51(a)
(On behalf of Plaintiffs and the California Subclass)

174. Plaintiffs incorporate by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

175. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

176. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

177. A "trap and trace device" is a "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

178. In plain English, a "pen register" is a "device or process" that records *outgoing* information, while a "trap and trace device" is a "device or process" that records *incoming* information.

179. Historically, law enforcement used "pen registers" to record the numbers of outgoing calls from a particular telephone line, while law enforcement used "trap and trace devices" to record the numbers of incoming calls to that particular telephone line. As technology has advanced, however, courts have expanded the application of these surveillance devices. This, combined with the California Supreme Court's mandate to read provisions of the CIPA broadly to protect privacy rights, has led courts to apply CIPA § 638.50 to internet tracking technologies similar to the Defendants' technologies at issue here. *See, e.g., Shah v. Fandom, Inc.*, --- F. Supp. 3d ---, 2024 WL 4539577, at *21 (N.D. Cal. Oct. 21, 2024) (finding trackers were "pen registers" and noting "California courts do not read California statutes as limiting themselves to

the traditional technologies or models in place at the time the statutes were enacted"); *Mirmalek v. Los Angeles Times Communications LLC*, 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024) (same); *Moody v. C2 Educ. Sys. Inc.*, --- F. Supp. 3d ---, 2024 WL 3561367, at *3 (C.D. Cal. July 25, 2024) ("Plaintiff's allegations that the TikTok Software is embedded in the Website and collects information from visitors plausibly fall within the scope of §§ 638.50 and 638.51."); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) (referencing CIPA's "expansive language" when finding software provided by data broker was a "pen register").

180. The Tracking Tools and other persistent cookies that Defendant installed on Plaintiffs' and California Subclass Members' browsers, to the extent they do not intercept "contents" of communications as defined in CIPA § 631(a), are "pen registers" because they are "device[s] or process[es]" that "capture" the "routing, addressing, or signaling information"—the IP address, geolocation, device information, and other persistent identifiers—from the electronic communications transmitted by Plaintiffs' and California Subclass Members' computers or smartphones. Cal. Penal Code § 638.50(b); *see also Shah*, 2024 WL 4539577, at *3; *Mirmalek*, 2024 WL 4102709, at *3.

181. At all relevant times, Defendant installed the Tracking Tools—which are pen registers—on Plaintiffs' and the California Subclass Members' browsers, which enabled Defendants to collect Plaintiffs' and the California Subclass Members' IP addresses, detailed URL requests, device information, and other persistent identifiers within the Website. Defendants then used the Tracking Tools and cookies to build comprehensive user profiles, which were used to unjustly enrich Defendant by linking and enhancing Plaintiffs' and the California Subclass Members' data to increase its advertising capabilities.

182. Plaintiffs and California Subclass Members did not provide their prior consent to

Defendant's installation or use of the Tracking Tools, cookies, and other tracking technology detailed herein.

183. Defendant did not obtain a court order to install or use the Tracking Tools, cookies, and other tracking technology detailed herein.

184. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and California Subclass Members have been injured by Defendant's violations of CIPA § 638.51(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 638.51(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure; naming Plaintiffs as representatives of the Class; and naming Plaintiffs' attorneys as Class Counsel to represent the Classes;

(b) For an order declaring that Defendant's conduct violates the statute referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class Members on all counts asserted

herein;

(c) For compensatory, statutory and punitive damages in amounts to be determined by the Court and/or jury;

(d) For prejudgment interest on all amounts awarded;

(e) For an order of restitution and all other forms of equitable monetary relief; and

(f) For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR TRIAL BY JURY

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable as of right.

Dated: January 31, 2025

Respectfully submitted,

GUCOVSCHI ROZENSHTEYN, PLLC

By: /s/ Adrian Gucovschi
Adrian Gucovschi, Esq.

Adrian Gucovschi
Nathaniel Sari (*pro hac vice forthcoming)*
140 Broadway, Suite 4667
New York, NY 10005
Tel: (212) 884-4230
adrian@gr-firm.com
nsari@gr-firm.com

Counsel for Plaintiffs and the Class